CLAIMS

What is claimed is:

1. A method, comprising:

   a.) receiving an IP packet at a network interface;

   b.) examining said IP packet to determine if IPSec processing is necessary;

   c.) performing IPSec processing on said IP packet;

   d.) transmitting said IP packet after IPSec processing to a storage location; and

   e.) performing TCP/IP processing on said IP packet in said memory location.

   f.) transmitting application data after said TCP/IP processing to a system memory

2. The method of claim **1** further comprising, examining the inbound IP packet at the network interface.

3. The method of claim **1** further comprising, examining the inbound IP packet at an acceleration device.

4. The method of claim **1** further comprising a queue which may receive IP packets awaiting IPSec processing.

5. The method of claim **1** further comprising a cryptographic acceleration device for performing IPSec processing on said IP packet requiring IPSec processing, wherein said IPSec processing does not utilize system memory, the system bus, or the chip interconnection network.

6. The method of claim **5** further comprising accessing a security policy database necessary for IPSec processing directly from the IPSec Decryption Accelerator, wherein said security policy database may exist in hardware, or said security policy database may exist in software.

7. A method as in claim **6** wherein a memory location may store overflow information from said security policy database.

8. A method as in claim **1** wherein said storage location comprises a Network Offload Memory (NOM).

9. A method as in claim **1** wherein said storage location comprises a temporary buffer.

10. A method as in claim **7** wherein said memory location comprises a system memory.

11. A method as in claim **1** wherein transmitting said IP packets after IPSec processing to said memory location comprises transmitting said IP packet by Direct Memory Access (DMA).

12. The method of claim **1** further comprising a TCP/IP processor or TCP/IP processors accessing said IP packet in said memory location, performing TCP/IP processing on said IP packet, and thereafter directing data resulting from said TCP/IP processing to a system interface.

13. A method as in claim **12** wherein TCP/IP processing on said IP packet by said TCP/IP processor or TCP/IP processors comprises accessing said IP packet by Direct Memory Access.

14. The method of claim **1** further comprising, transferring said data resulting from said TCP/IP processing to a system interface by Direct Memory Access (DMA).

15. The method of claim **1** further comprising receiving an IP packet which was transmitted in tunnel mode, or receiving an IP packet which was transmitted in transport mode.

16. A method, comprising:

a.) receiving data from the system;

b.) performing TCP/IP processing on said data, creating an IP packet;

c.) processing said IP packet to determine if IPSec processing is necessary and directing said IP packet to an accelerator for IPSec processing;

d.) performing IPSec processing on said IP packet; and

e.) transmitting IP packets at a network interface;

17. The method of claim **16** further comprising a system interface for receiving data from said system, which may be a CPU.

18. The method of claim **16** further comprising transmitting said data received from said system to a memory location.

19. A method as in claim **16** wherein said memory location comprises a Network Offload Memory (NOM).

20. A method as in claim **16** wherein said memory location comprises a system memory.

21. The method of claim **16** further comprising transmitting said data received from said system by way of Direct Memory Access (DMA) to said memory location.

22. The method of claim **16** further comprising a TCP/IP processor or TCP/IP processors for performing TCP/IP processing.

23. The method of claim **16** further comprising accessing said data for TCP/IP processing by way of Direct Memory Access(DMA).

24. The method of claim **16** further comprising the TCP/IP processor or TCP/IP processors checking the IP packet after TCP/IP processing to determine if IPSec processing is required on said IP packet.

25. The method of claim **16** further comprising a queue which may receive IP packets awaiting IPSec processing at said accelerator.

26. The method of claim **15** further comprising setting a control bit in a control word for a DMA engine to notify said accelerator that said IP packet requires IPSec processing.

27. The method of claim **26** further comprising said accelerator checking said control bit to determine if IPSec processing is required on said IP packet.

28. The method of claim **26** further comprising said DMA engine checking said control bit to determine if IPSec processing is required on said IP packet.

29. The method of claim **28** further comprising said DMA engine sending only packets which require IPSec processing to said accelerator.

30. The method of claim **28** further comprising said DMA engine sending packets which do not require IPSec processing to said network interface.

31. The method of claim **16** further comprising a network interface for receiving said IP packet after IPSec processing, and for said network interface receiving IP packets which do not require IPSec processing.

32. The method of claim **16** further comprising transmitting an IPSec packet in tunnel mode, or transmitting an IP packet in transport mode.

33. An apparatus comprising:

a.) a network interface or network interfaces, said network interface or network interfaces receive and send IP packets;

b.) an accelerator or accelerators coupled to said network interface or network interfaces, said accelerator or accelerators perform IPSec processing on inbound IP packets, and/or perform IPSec processing on outbound IP packets;

c.) a TCP/IP processor or TCP/IP processors coupled to said network interface or network interfaces, said TCP/IP processor or TCP/IP processors perform TCP/IP processing; and

d.) a system interface or system interfaces coupled to said TCP/IP processor or TCP/IP processors, said system interface or system interfaces receives and/or sends data from a System CPU.

34. The apparatus of claim **33** further comprising a single device or multiple devices.

35. An apparatus as in claim **33** wherein said apparatus comprises:

a.) an inbound network interface, said inbound network interface receives inbound IP packets from a network;

b.) an accelerator coupled to said inbound network interface, said accelerator receives an IP packet from said inbound network interface and performs IPSec processing on said IP packet;

c.) a security policy database (SPD) coupled to said accelerator;

d.) a security association database (SAD) coupled to said accelerator;

e.) a chip interconnection network coupled to said accelerator;

f.) a memory coupled to said chip interconnection network;

g.) a TCP/IP processor coupled to said chip interconnection network; and

h.) a system interface coupled to said chip interconnection network.

36. An apparatus as in claim **35** wherein said inbound network interface comprises an Ethernet interface.

37. The apparatus of claim **35** wherein said accelerator is an IPSec Decryption Accelerator, wherein said IPSec Decryption Accelerator does not utilize system memory, the system memory bus, or a chip interconnection network.

38. The apparatus of claim **35** wherein said transmission between said accelerator and said memory location is comprised of Direct Memory Access (DMA).

39. The apparatus of claim **35** wherein said connection between said memory location and said TCP/IP processor is comprised of Direct Memory Access (DMA).

40. The apparatus of claim **35** wherein said connection between said memory location and said system interface is comprised of Direct Memory Access (DMA).

41. An apparatus as in claim **33** wherein said apparatus comprises:

a.) a system interface for receiving data;

b.) a chip interconnection coupled to said system interface;

c.) a TCP/IP processor coupled to said chip interconnection network;

d.) a memory coupled to said chip interconnection network;

e.) an accelerator coupled to said chip interconnection network;

f.) a security policy database (SPD) coupled to said accelerator, and said security policy database coupled to said TCP/IP processor;

g.) a security association database (SAD) coupled to said accelerator, and said security association database coupled to said TCP/IP processor;

h.) an outbound network interface coupled to said accelerator;

42. The apparatus of claim **41** wherein said system interface may transmit said data by Direct Memory Access (DMA) to said memory location.

43. The apparatus of claim **42** wherein said memory location is comprised of Network Offload Memory (NOM).

44. The apparatus of claim **42** wherein said memory location may be a system memory.

45. The apparatus of claim **41** wherein said TCP/IP processor may access said data in said memory location by Direct Memory Access (DMA).

46. The apparatus of claim **41** wherein said data in said memory location may be transmitted by Direct Memory Access (DMA) from said memory location to said accelerator after TCP/IP processing.

47. An apparatus as in claim **41** wherein said accelerator comprises an IPSec encryption accelerator, wherein said IPSec encryption accelerator does not utilize system memory, memory bus, or a chip interconnection network.

48. The apparatus of claim **41** wherein said security policy database may be a hardware location, or said security policy database may be a software location.

49. The apparatus of claim **41** wherein a memory location may store overflow information from said security policy database.

50. The apparatus of claim **49** wherein said memory location may be Network Offload memory (NOM).

51. The apparatus of claim **49** wherein said memory location may be a system memory.